South Hams District Council ICT Security Policy (including hardcopy data storage security)

Policy Owner: ICT Manager
Policy Sponsor: Corporate Management Team
Policy Ratification: SHDC Executive

Version	Activity	Who	Date
0.1	Initial research and draft	S Landfear	October 2001
0.2	Review and further drafting	R Barlow	May 2002
0.3	Updates resulting from 'Joint Staff Consultative Forum', and continuing updates to the Service provider section	R Barlow	June 2002
0.4	Service provider section re-vamped	R Barlow	September 2002
0.5	Updates resulting from review by Internal Audit	R Barlow	October 2002
1.0	Distributed for CMT approval	R Barlow	October 2002
1.1	Updates from Graham Rowe and Mark Seymour	R Barlow	November 2002
1.2	Distributed for CMT approval	R Barlow	November 2002

Next review: *(12 months from this final draft)*

Abstract

This policy document is a formal statement on the Council's policy towards the security of Council ICT hardware, software, data and intellectual property related assets. This policy addresses the requirements and responsibilities of the management at all levels within the organisation, the users of the ICT facilities and the ICT service providers (in the main the SHDC ICT Section). This policy must be supported by the Council's Executive and the Corporate Management team. The key areas addressed in this policy are:

SHDC Management :

- Management responsibilities to support this policy at all levels, and take appropriate action where there is an identified breach;
- Management to take responsibility for the data used by the Council, and to ensure appropriate controls are in place to meet the relevant legislation, in particular the 1998 Data Protection Act, which covers data held on both ICT systems and hardcopy;

Users :

- General User responsibilities and allowable activities when using the Council ICT equipment;
- The importance of the passwords, especially as the Council moves to meet its e:government objectives;
- The importance of maintaining data integrity and confidentiality, including the policy of not providing database creation tools.
- The importance of managing the installation of software or data on ICT equipment, both to ensure the Council is not liable by breaching external Copyrights, and to reduce the cost to the Council of supporting ICT equipment;
- Reducing the likelihood of loss of vulnerable equipment or confidential data where ICT equipment is outside the normal office environment;
- Reducing the potential for external access to the SHDC ICT network, and potentially fraud or malicious damage;

ICT Section and third party service providers:

- Systems controls, including the desktop 'lock down' policy to minimise inappropriate use and reduce overall ICT support costs
- Availability management, including the regular system backups and facilities to recover the systems in an emergency
- Network security controls to limit inappropriate activities and minimise the likelihood and impact of malicious software (viruses);
- Software development security requirements, including the controls around data access;

Where applicable, local operational requirements may need to vary this policy. In all situations, this variation must be agreed with the ICT Section and Internal Audit as a minimum.

1 Introduction 4
1.1 Objectives 4
1.2 Key definitions 4
1.3 Scope 5
1.4 Legislation and other policy 6
1.5 Security Triangle 6
2 Management Responsibilities 7
2.1 Application of the Policy 7
2.2 Management of SHDC held data 7
2.3 Management of SHDC ICT systems 8
2.4 Management of Business Continuity plans 9
3 User responsibilities 10
3.1 Ethics 10
3.2 Acceptable Use 10
3.3 Password Policy 11
3.4 Data integrity and confidentiality 13
3.5 Software and data Installation 13
3.6 ICT Equipment 14
3.7 Use of vulnerable Council owned equipment 14
3.8 Use of non-Council equipment within the Council environment 15
3.9 Use of non-Council equipment outside the Council environment 16
3.10 Access to Council facilities by non-Council Representatives. 17
4 ICT provider responsibilities 18
4.1 Asset Administration 18
4.2 Physical Security 18
4.3 Security administration 20
4.4 Asset Access Controls 20
4.5 Access Accounts and Groups 21
4.6 ICT Service Continuity 23
4.7 Change Management and Release Management 24
4.8 Server Management 24
4.9 Network Infrastructure Management 26
4.10 Inter-network Connection Management 27
4.11 Wide Area Network Connection Management 28
4.12 Local Area Network Connection Management 29
4.13 Local Area Network User Access Management 29
4.14 Proactive asset monitoring and management 30
4.15 System development and third party product selection 31
4.16 Miscellaneous requirements 32
4.17 Accountability and audit 33
4.18 Security Breach Management 34
Appendix A – Acceptable use 35
Appendix B - Data and Information Classification 38
Appendix C - Guidance creating a secure password 39
Appendix D – Security policy overview 40

The Security Policy outlines Security policies and procedures, why they are needed and considered to be important, plus explanations as to what is and what is not allowed with regards to the Council. The policy has been written to be general enough that changes should not have to be made to the policy outside of the review period documented in the policy. It contains general directives, which are not overly architectural, and system dependent. The Policy tackles application of the policy i.e. it should be clear what disciplinary measures are to be expected if the policy is breached by a user in the Council.

1 Introduction

1.1 Objectives

South Hams District Council seeks to maximise the availability and integrity of its ICT Systems. It also must control costs, both in the delivery of the ICT Service, and damages sought from licensing or legislation breaches. Security management underpinned by an agreed Security Policy must be in place to meet these objectives. The security policy should ensure:

1.1.1 the Council's assets are secured against loss by theft, fraud, malicious or accidental damage, or breach of privacy or confidence. This includes the disclosure of physically stored data/information (paper etc), as covered by the 1998 Data Protection Act

1.1.2 The Council is protected from damage or liability resulting from use of its facilities for purposes contrary to existing legislation or Council policy;

1.1.3 The Council is protected from damage or liability resulting from the use of ICT facilities not belonging to the Council, but being used to support the activities of the Council.

1.2 Key definitions

Throughout this policy, various terms are used frequently. These are:

Account — A unique sequence of characters and numbers that is used to 'log on' to an ICT system. When accompanied by a password, this can used to identify a particular user (and in some cases can represent a legally enforceable digital signature)

Council representatives — This covers any SHDC Council employees, SHDC Members and personnel under the direction of SHDC employees.

Data — This covers both 1) raw measures, statuses and results, for example from surveys; 2) refined information, either from the analysis of data or direct facts, for example a name of a property.

ICT — **I**nformation and **C**ommunication **T**echnology. The combination of computing (hardware and software), data and telecommunications (telephone and computer network) techniques and technologies.

ICT Equipment	Any device capable of being linked to the current SHDC Computer or telephone equipment for the purpose of data transfer. The link may be direct (wire, infrared, radio link) or indirect (via an intermediary device, for example Car Park meters to a hand held device, which is then transferred to a standard SHDC computer)
ICT Security	This refers to the processes and procedures in place to ensure that the ICT infrastructure (including hardware, software and data) is managed to ensure their confidentiality, integrity and availability is not compromised and that the Council is not put at risk through inappropriate use of the Infrastructure.
ITIL	Information Technology Infrastructure Library. Office of Government Commerce (OGC) sponsored ICT Management best practice being deployed at SHDC
Service User	This refers to any Council Representative who makes use of any of the Council's ICT facilities or uses externally provided facilities. Also referred to as *User*
Service provider	This refers to the External or Council organisation responsible for supporting and maintaining the service provision to the Service Users. On the whole for the majority of the Council ICT (Information and Communications Technology) systems, this can be interchanged with the ICT Section.
SHDC Management	The group of responsible officers, comprising both the Chief Officers and Service Centre Managers

1.3 Scope

The policy covers:

- All users of the Council's computer network
- The deployment and use of the Council's electronic information systems (i.e. all computers, peripheral equipment, software and data) within Council property, or belonging to the Council, but located elsewhere.
- The use of information systems not owned by the Council and located outside of its property, where such use is effected from or via equipment located on Council property, or by equipment belonging to the Council;

- The use of information systems not owned by the Council or located on its property, but used by Council staff for business purposes connected with the Council.

- The security of hardware, software and data; the security of personnel using information systems; and the security of the Council's assets that may be placed at risk by misuse of information systems.

- All Data Protection issues where any Council activities make use of personal or sensitive personal data no matter whether it is stored on an ICT system or in an alternative physical system for example on paper or microfiche.

1.4 Legislation and other policy

The Policy is to be read in the context of the following information:

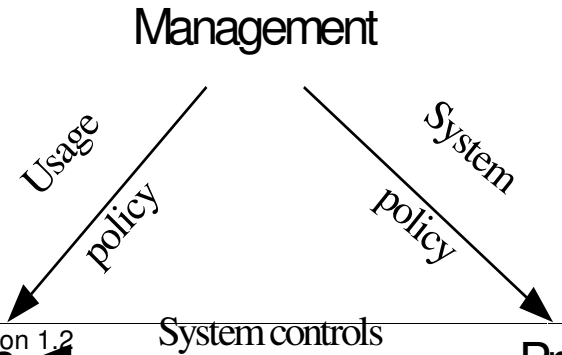
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1998
- The Copyright (Computer Programs) Regulations 1992 (SI 3233)
- ISO17799 (BS7799), the security standard
- Freedom Of Information Act 2000
- SHDC Financial Regulations
- Code of Conduct for Members

It should be noted that due to conflicting requirements of the above legislation and standards, this Policy will need to be reviewed when clarification results from case law or other means. Where a conflict arises between this policy and the above information (1.4) , the above information (1.4) will take precedent.

1.5 Security Triangle

For effective ICT security, there are usually three main parties:

- Management, who need to set the policies and ensure these are being followed;
- Service providers, who provide the ICT systems and who deploy system controls to limit the activities that might cause security breaches;
- Users, who use the systems, governed by



the policies and guided by the system controls in place.

This policy addresses all three areas.

2 SHDC Management Responsibilities

2.1 Application of the Policy

Awareness: Through relevant education and training, it is the responsibility of the *SHDC Management* to ensure that all Service Users and Service providers are aware of their responsibilities in regard to this policy.

Enforcement: It is the specific responsibility of *SHDC Management* to ensure that the Policy is carried out. All Service Users and Service providers have a personal responsibility to ensure that they, and others who may be responsible to them are aware of and comply with the Policy.

Breach: It is the duty of the SHDC ICT Manager to take appropriate action to prevent breaches of the policy. Where such action is outside of the remit of the ICT Section, the appropriate Chief Officer will be responsible for ensuring appropriate processes and procedures are deployed and regularly reviewed.

Service Users and internal Service providers who do not adhere to this policy will be dealt with through the Council's disciplinary process. For Councillors, the Member & Administrative Support Manager in association with the Chief Executive will ensure appropriate action is taken. Where Service providers breach the policy, this should be addressed contractually.

Review: *SHDC Management* will be responsible for regular reviews of the Policy in the light of changing circumstances.

2.2 Management of SHDC held data

The data held within the Council is one of the most important corporate assets. This policy covers all aspects of data to directly support the working of the ICT systems and to support the non-ICT supported Council activities, for example documentation of procedures. In addition, with the tightening of the legislation for the holding of personal and sensitive personal data, the control of this resource must be considered an *SHDC Management* responsibility. *SHDC Management* must therefore ensure:

2.2.1 that all potentially personal, confidential or important data assets are assigned an owner;

2.2.2 the owner classifies the data into one of the classification levels (listed in *Appendix B*), depending on Council policies (including Data Protection and Freedom of Information), legislation and business needs;

2.2.3 the owner specifies who is allowed access to the data;

2.2.4 the owner is responsible for this data and shall implement appropriate controls according to its classification;

2.2.5 the owner is responsible for ensuring adequate controls are provided to ensure the integrity of the data meets its quality requirements;

2.2.6 the owner provides processes to review the relevance of the data being stored, and where necessary take actions to dispose of any redundant data. This must consider Data Protection issues as to the length that personal data should be held without re-acquiring consent to hold it;

2.2.7 that where data is to be disposed of, the disposal process considers the sensitivity of the data, and ensures that where necessary all copies of this data are disposed of;

2.2.8 that where users are likely to come into contact with confidential data, a suitable confidentiality clause is included in the job description to form part of the contract of employment. For Councillors, this is covered in the 'General obligations' section of the *South Hams District Council Councillor's code of conduct;*

2.2.9 that where *new*, potentially personal data is to be stored on paper or electronically, the Council's data protection registrar must be notified in writing of the type of information and it's purpose.;

2.2.10 that suitable processes are in place to ensure that business critical data is protected from loss to ensure business continuity;

2.2.11 that there is a regular review of points 2.2.1 through to 2.2.10.

To support this policy, multi-user database tools will not be provided for use. Where a multi-user database tool is required, this should be requested through the ICT Section, who will provide a solution that meets the requirements laid out in this policy

2.3 Management of SHDC ICT systems

Access to the ICT systems must be managed. This is usually technically accomplished through the use of physical and password controls, but this can only be effective if there are suitable processes in place to manage who should be given access to a particular system and what parts of that system should be available. *SHDC Management* therefore have the responsibility to ensure:

2.3.1 that all ICT systems have a designated system owner who is responsible for ensuring the level of security controls for the system meets the Council's or external entities security requirements;

2.3.2 that an ICT Access Request is completed for any additional system access for a user, and that this is authorised by the users appropriate line manager (Service Centre managers and above).

For Councillors, this will either be agreed with Member and Administrative Support Manager, or the Chief Executive;

2.3.3 that the ICT Access Request is secondly authorised by the system owner, who will also be expected to define the exact level of access to be provided;

2.3.4 that the user is only provided with the additional access after the ICT Access request is fully authorised;

2.3.5 that processes are in place to regularly review the access requirements for users, taking special consideration of those whose duties have changed;

2.3.6 that processes are in place to ensure that the system access is revoked where a User is no longer with the Council, or frozen, where the user is to be away for an extended period, for example maternity or sick leave;

2.4 Management of Business Continuity plans

With ICT being so critical to the functioning of the Council, *SHDC Management* must ensure that a Business Continuity Strategy is in place that:

2.4.1 identifies vital business functions (VBF) that are dependent on the ICT systems;

2.4.2 identifies key threats to these VBFs;

2.4.3 identifies appropriate recovery requirements for each VBF;

SHDC Management must ensure that appropriate ICT Continuity and Recovery plans are deployed to support the Business Continuity Plan. This policy recommends that all ICT Continuity plans are managed through the SHDC ICT Manager. All plans should be regularly reviewed and where appropriate tested.

3 User responsibilities

Training and education of the users' in respect to their responsibilities towards the security of the organisation is key to the success or failure of a security policy. No level of technical barriers can overcome the inconsistencies of human behaviour. It is therefore necessary to ensure that the people involved in any of the processes are aware of their responsibilities, and also the consequences of not carrying these duties out. Suitable controls should also be deployed to assist in this clarification and adherence, for example a separation of duties for certain tasks.

3.1 Ethics

Users are:

3.1.1 NOT allowed to use the Council's computer equipment for private purposes unless authorised by the relevant Service Centre Manager or Chief Officer, and only then in exceptional circumstances and under strict conditions and guidelines. The use of the Council's e-mail system can however be used for reasonable private use on a strictly occasional basis (for the avoidance of doubt, five or less incoming or outgoing private e-mails per week are considered occasional);

3.1.2 NOT allowed to attempt to crack systems; run password checkers on system password files, run network sniffers, break into other accounts, disrupt service, abuse system resources, misuse e-mail, examine other users files unless asked to do so by the file owner;

3.1.3 NOT allowed to attempt to circumnavigate security controls, for example determine a method to avoid the inactivity screen timeout activating;

3.1.4 NOT allowed to download or copy executable programs (e.g. files with the extension *.exe *.com *.VBS *.BAT etc);

3.1.5 NOT allowed to download or copy data that may infringe licensing or Council policy;

3.1.6 NOT allowed to configure, disassemble, modify, reset or reposition any ICT equipment except where specifically authorised to do so;

3.1.7 to take appropriate security precautions in respect of computers under their control;

3.1.8 requested not to consume food or drink near ICT equipment;

3.1.9 responsible for all damage to equipment, software or data resulting from failure to observe this policy, potentially resulting in disciplinary action.

3.2 Acceptable Use

Two related policies described what South Hams District Council considers acceptable use of ICT Equipment and systems. This has now been replaced with the one guide, included in Appendix A. This should be made available on the intranet, which should always contain the definitive version.

3.3 Password Policy

The combination of username and password define the identity of users on a system. With the requirements of e.government and efficiencies to be gained from automating paper based processes, the password may replace the current use of written signatures. It will therefore be increasingly important to ensure that only the authorised person knows their password. A good personal password policy is the most important barrier to unauthorised access in current systems.

Passwords must:

3.3.1 NOT be written down; put on the wall; kept in a drawer, e-mailed etc;

3.3.2 NOT be given to others. No-one should ask users for their passwords, even the ICT Section. Any such requests should immediately be reported to the users' line management;

3.3.3 be IMMEDIATELY changed if they have been disclosed or there is a suspicion they have been compromised;

3.3.4 be CHANGED regularly.

Users are:

3.3.5 NOT allowed to access computer systems using another users' login and password. You must not use anyone else's account and password or disclose your own;

3.3.6 NOT allowed to share accounts or passwords with colleagues unless explicitly agreed in writing with SHDC Internal Audit, the ICT Manager and the appropriate users' Chief Officer, or in the case of Councillors, the Chief Executive.

3.4 Levels of system security

Ideally, a password should only be used on one system at a time, and therefore for some users, it would be necessary to remember many (different) passwords. In reality, for most people it is difficult to remember more than a handful, and therefore there is a tendency to want to re-use the same password for each system. This brings risks as different systems have different levels of security, generally based on the type of data held.

A password is only as secure as the least secure system it is used on.

To avoid compromising the SHDC systems, five types of system have been defined, with password requirements for each.

Type	Description	Password requirements
1	Internal systems recognised for having secure access	Minimum 6 characters, preferably 8 or more (letters and numbers). Each password must be more than three characters different than the last. Passwords must not be reused on another level 1 system after it expires. Passwords to be changed monthly.
2	Internal systems with unknown security but containing sensitive, personal or confidential data	Minimum 6 characters, preferably 8 or more (letters and numbers). Passwords must not be reused on another level 2 system for six months after it expires. Passwords to be changed monthly.
3	Low Security internal systems	Minimum 4 characters. Passwords must not be reused on another level 3 system for two months after it expires. Passwords to be changed monthly.
4	External hosted/ Internet systems	Minimum 6 characters. Passwords must not be reused on another level 4 system for two months after it expires. Passwords to be changed monthly. This is a guide as each system will be different.
5	External facing systems (hosted by SHDC)	A special category, usually used in the technical systems that manage external access to the council LAN. Minimum 10 characters letters and numbers. The password duration will depend on the access controls and access monitoring in place.

It is envisaged that the majority of SHDC systems will be type 1, as they are accessed using the 'Windows NT' or 'Unix' passwords.

Appendix C provides more guidelines for passwords.

The classification of the SHDC systems are defined on the Intranet <location to be provided>

A password MUST NOT be used or re-used on a more secure system after or during the time it is used on a less secure system.

3.5 Data integrity and confidentiality

To carry out its duties, the Council is responsible for a significant amount of data. Much of this data is personal or confidential, and therefore care must be taken to ensure the integrity and confidentiality is maintained at all times. Section 2.2 has covered the responsibilities for *SHDC Management* to identify and classify all data used by the Council, and also to implement suitable security controls.

Therefore users:

3.5.1 Must comply with the security controls;

3.5.2 Where security controls are not evident or provided, the user must **consult** with their service centre manager and the ICT Section **before** carrying out any of the following activities with data:

- 3.5.2.1 entering the data into an alternative internal data store, where the use of the data store is not fully understood;
- 3.5.2.2 entering the data into any external data store, whether verbally, written or electronically – this includes external surveys, internet forums and product registrations;
- 3.5.2.3 transferring the data outside the confines of the SHDC locations whether written or electronically.
- 3.5.2.4 disposal of data;
- 3.5.2.5 creating data repositories, whether electronic or paper based that stores information that might be considered personal or confidential or important for the functioning of Council business;

3.5.3 Must NOT provide any data to non-Council representatives without the express permission of the Chief Officer who has taken responsibility for the data. Where legislation provides powers of access to external organisations, the access should be granted, with the Chief Officer being notified immediately;

3.5.4 Must follow agreed procedures when adding, amending or deleting Council held data to ensure the integrity meets the quality requirements.

3.6 Software and data Installation

Unauthorised installation of software or its supporting data on the Council's computer systems:

- significantly increases the cost of supporting the Council systems;
- potentially will lead to large fines and imprisonment of Council officers;
- risks the Council data / systems if the software turns out to be malicious.

Therefore users:

3.6.1 are NOT permitted to load software via any method (floppy diskette, CD-ROM; USB; Internet download etc). This includes updates to software already installed;

3.6.2 are NOT permitted to load data via any method (floppy diskette, CD-ROM; USB; Internet download etc). This includes updates to data already installed, but where there is a need to use specific data (for example clip art or CD based catalogues), data loading may be agreed with the ICT Section;

3.6.3 must request all software loading from the ICT Section.

To assist adherence to this policy, all routes to externally install software are barred including the 'A' drive, 'C' drive and CD-ROM drive, and content filtering and monitoring for e-mail and the Internet is carried out.

3.7 ICT Equipment

To ensure the compatibility, suitability, cost effectiveness, maintainability, security and safety of ICT equipment, the ICT Section are responsible for the procurement, installation and subsequent relocation of Council Owned ICT equipment. The only activities users should be involved in are:

3.7.1 simple user maintenance, which is usually specified in the accompanying user manual, including for example changes of toner cartridges;

3.7.2 purchase of consumables for ICT equipment unless otherwise advised;

3.7.3 switching ICT equipment off at the mains switch when not in use, reducing the risk of fire, and supporting the Council's environmental policy.

> ***Note*** *it is not usually enough to switch off ICT equipment with the switch on the equipment as most modern equipment only partially switches off when this is used.*

3.8 Use of vulnerable Council owned equipment

Vulnerable equipment tends either to be portable equipment or equipment in a low security environment, for example a reception area. The main risks are:

- accidental or malicious damage, especially to portable equipment like Laptop computers that are less robust than desk based computers;
- theft, especially for portable equipment, with potentially no insurance cover;
- disclosure of personal or confidential data due to them being operated in an external less controlled environment;

- unauthorised point of access to Council systems through lack of supervision of an accessible and connected computer.

Therefore users:

3.8.1 are to only use laptops agreed and provided by the ICT Section;

3.8.2 must request a data encryption mechanism to be installed if the vulnerable equipment will need to hold personal or confidential data and/or be used to transmit or receive such data over a public network (telephone system);

3.8.3 must ensure that computer screens are not visible to non-Council representatives unless it is known that the data displayed is non-sensitive;

3.8.4 must NEVER store passwords on vulnerable equipment;

3.8.5 are to ensure automatic screen locking mechanisms and other security mechanisms are used as agreed with the ICT section;

3.8.6 are responsible for vulnerable equipment whilst outside the building and should take reasonable steps to ensure the security of the equipment;

3.8.7 must carry laptops in a carry case on public transport;

3.8.8 must switch off the equipment when not in use, including the modem and monitor screen;

3.9 Use of non-Council equipment within the Council premises

There will be times where users may need to bring personal or third party ICT equipment onto the Council premises. This brings the following risks:

- Electrical safety
- Compatibility with Council equipment
- Insurance

Therefore users:

3.9.1 must notify the relevant site manager of any electrical equipment that needs to be connected to the mains electricity as it must be electrically tested;

3.9.2 must NOT attempt any kind of connection between the equipment and any of the Councils ICT equipment (including the phone system and network);

3.9.3 must request the ICT Section to carry out a compatibility assessment if there is a need to connect it, and depending on the outcome, an appropriate course of action will need to be agreed;

3.9.4 must for non-standard equipment check with the Council's insurance representative to confirm that the use of the equipment will not void any of the building or liability cover.

3.10 Use of non-Council equipment outside the Council environment

There will be times when users need to carry out Council activities on systems that are not owned or controlled by the Council. This is particularly pertinent for Councillors and senior officers in the Council who may carry out work in the evenings on documents and spreadsheets.

The main risks of this are:

- unlicensed software and/or data being used on home computers for Council work, which could potentially result in license issues and fines;
- the introduction of computer viruses when work is returned to the work environment;
- disclosure of confidential or personal data held on non-secure home computers;
- transmission of confidential or personal data over the public network to and from the home computer;
- Reduction in security controls, for example few home computers will lock the screen after a period of inactivity, potentially leaving the Council work insecure.

This policy specifies that users:

3.10.1 confirm that the software and data on their home computer is fully licensed if this is needed to carry out the work, (including the operating system software for example Windows 98, Windows XP);

3.10.2 should have up to date virus checking software on their computers, to reduce the risk of introducing viruses back to the Council. This is a recommendation for all computer users to protect their own computers;

3.10.3 must NOT transfer confidential or personal data to a non-Council computer. The need to use such data will require the use of a Council provided computer to ensure the necessary controls are in place;

3.10.4 activate access controls where possible, for example Microsoft Windows password protection, this should be implemented to provide some level of access control to the computer files. The password policy and guidelines apply in this situation.

The new DASH system (Direct Access South Hams) will provide a secure mechanism to access the systems directly from homes into the central Council network, which is likely to increase the number of staff wishing to work from home, but will introduce additional security risks.

Users wishing to use the new DASH direct access system will need to confirm in writing that the following usage restrictions will be adhered to. These are that the remote computer:

3.10.5 must have active and up to date virus checking installed on the computers used to access DASH, as this is needed to detect and remove trojans that could gather passwords as they are typed;

3.10.6 must not be using any password assistance tools (e.g Gator), which stores passwords – these have been shown to both pass back passwords to external companies and allow other programs to discover the passwords;

3.10.7 must only use the system from the security of their normal residence or where necessary hotel accommodation. On no account should this be used in a public venue, for example an Internet Café;

3.10.8 must ensure that the computer is never left unsupervised whilst logged onto the DASH system;

3.11 Access to Council facilities by non-Council Representatives.

In the event that there is a requirement to provide non-Council representatives access to Council computers, this must be discussed on an individual basis with the ICT Section, who will then co-ordinate other discussions with the relevant Council parties to determine an appropriate response. The policy is therefore that NO ACCESS should be provided to Council computer systems for non-Council representatives.

4 ICT provider responsibilities

The ICT provider will support the *SHDC Management* and User policy requirements with suitable processes and procedures.

To ensure the security of ICT Assets, which include ICT Hardware, software and intellectual property, controls should be put in place to fully account for, maintain and secure these assets.

4.1 Asset Administration

The ICT provider must :

4.1.1 maintain the following related information for each asset:

ownership; maintenance; licence; contract; supplier; installed location; data classification; Network addresses (IP & MAC)

4.1.2 ensure all ICT assets are recorded for insurance and financial purposes;

4.1.3 ensure all computing devices that are installed are labelled;

4.1.4 meet Health and Safety recommendations in ensuring:

4.1.4.1 all wiring is neat and tidy and labelled such that a connection may not be accidentally disturbed or broken;

4.1.4.2 all electrical ICT devices that connect to the 'mains' are electrically tested;

4.1.5 ensure the disposal of ICT assets are controlled via an auditable process, in accordance with the SHDC Financial Regulations. Special attention must be taken to avoid potential liabilities regarding electrical safety and confidential data;

4.1.6 ensure new or changed systems have one of the security levels (documented in 3.3) allocated against them;

4.1.7 provide mechanisms to backup data held on remotely used assets.

4.1.8 where assets are acquired (whether purchased or not), they must be assessed for compatibility with the existing ICT Infrastructure. This should be carried out in a 'test environment', separated from the production infrastructure. Where there are issues with the compatibility, this must be referred to the ICT Manager for authorisation to proceed;

4.1.9 where assets are acquired (whether purchased or not), they must be assessed for compatibility with this security policy. Where there are issues with the compatibility, this must be referred to the ICT Manager and internal audit as a minimum for authorisation to proceed;

4.2 Physical Security

The ICT provider must ensure:

4.2.1 higher cost or desirable items are marked to be identifiable as SHDC property and to be uniquely marked;

4.2.2 where an asset is stored or can be physically secured, appropriate means should be taken to provide security of the asset;

4.2.3 controls are in place to record the location of ICT equipment, and especially to record when equipment is removed to a non-SHDC location;

4.2.4 where equipment is used in a publicly accessible place, the risks of this are understood, and any required mitigation actions taken;

4.2.5 regular risk assessments are undertaken to review the arrangements in place and incidents in the previous period.

In addition to these general requirements, specific measures should be taken depending on the actual location and type of equipment, including:

Area **Special Attention**	**Computer room**	**Network distribution points and PABX room**	**ICT Section office**	**User offices**	**Public Areas**
Access restrictions	√	√	√		
Electrical supply	√	√			
Temperature	√	√			
Humidity	√	√			
Fire suppressant	√				
Particulates (Dust etc)	√				
Key network cabling			√	√	√
IT Workstations					√

Access restrictions	Physical barring of access to area through the use of electronic or manual locks. Access should be managed to key staff who need regular access to these areas
Electrical supply	Equipment should be protected from both interruptions/spikes in the electrical supply, with key electrical feeds and isolators protected from accidental and malicious damage.
Temperature	Temperature should be monitored to ensure the temperature is kept within operating requirements, and where necessary appropriate action taken to maintain this temperature range.
Humidity/Water	Humidity should be monitored to ensure this is kept within the operating requirements, and where necessary appropriate action taken to maintain this. Drinks or liquids should not be taken / stored in these areas.
Fire suppressant	For key equipment, additional specialist fire suppressant systems (to BS Standard) should be installed, as normal office (water based) systems are not appropriate.

	Combustible materials MUST NOT be stored in these areas.
Particulates (Dust etc)	Dust particles reduce the life of computer equipment, and can also trigger false alarms in fire monitoring systems. Where appropriate, measures should be taken to minimise particulates, and where cleaning implements (vacuums) are used, these should be fully filtered (Hepa).
Key network cabling	Critical cabling that supports the 'back bone' of the ICT Network and telephony must be protected from accidental and malicious damage. Where possible this should be routed out of sight and reach, and where this is not possible, protected dependent on the assessed risk.
IT Workstations	These are considered vulnerable equipment wherever there is public accessibility. Physical security and visual deterrents (visible marking, CCTV, staff in close proximity)

4.3 Security administration

This policy by it's nature has to be reasonably generic. Where applicable, local operational requirements may need to vary this policy, this must be agreed with the ICT Section and Internal Audit as a minimum. Therefore, the ICT provider must:

4.3.1 ensure all variations are agreed by the required signatories;

4.3.2 maintain auditable records of all agreed and rejected variation requests;

4.3.3 review the variation requests on a regular basis to ensure these are still required;

4.3.4 as part of the regular security policy review, determine whether the policy should be modified in light of the variation requests.

4.4 Asset Access Controls

The controls are in place to ensure that assets or parts of assets are only used by users who are authorised to do so. These controls are usually used through Accounts. The ICT provider:

4.4.1 must enforce agreed access rights, and where appropriate an audit trail of successful and unsuccessful activities should be recorded;

4.4.2 should manage the available access points into key systems (for example only allowing the Unix root login available within the computer room);

4.4.3 must manage access to council data held on remotely used equipment, preferably using full encryption of this data;

4.4.4 should where required provide a mechanism to restrict the use of certain assets to particular time periods;

4.4.5 must ensure that controls and authorisations are kept current, for example where an upgrade to a software package occurs;

4.4.6 should ensure users are not be able to view the Access Control rights assigned to other users;

4.4.7 must ensure the users are informed of actions that violate security;

4.4.8 must ensure that the documentation of controls and authorisations are current and accurate.

The ICT provider must ensure changes to these controls and user authorisations:

4.4.9 have been authorised by the appropriate responsible officer (s) (usually Service Centre or Chief Officer level);

4.4.10 do not impact other users of the ICT systems

4.4.11 are recorded, and should include as a minimum:

asset(s); user(s); proof of authorisation; details of control / authorisation change; date/time of change

4.5 Access Accounts and Groups

To manage the controls that apply to each user on each asset, these are normally bound into a user **account** that is effectively the container that holds all relevant controls and the levels for that user on each asset. **Groups** may also be created that are collections of controls that can be attached to accounts. From a user perspective, accounts are normally seen as their 'login name'. The ICT provider must:

4.5.1 ensure each account and group is identified by a unique name and/or number;

4.5.2 ensure each account is authorised, and the controls and groups correctly maintained for each account;

4.5.3 identify the user of each account. Where an account is to be used for more than one user or the users are not known (for example Guest accounts), the ICT provider must ensure that authorisation is also obtained from Internal Audit, the ICT Manager and the appropriate user's Chief Officer, or in the case of Councillors, the Chief Executive;

4.5.4 be the primary administrator for all accounts, groups and controls. Where there is a business requirement for the users to do this, the ICT provider must ensure that authorisation is also obtained from Internal Audit, the ICT Manager and the appropriate user's Chief Officer. In all scenarios, the ICT provider must have administrator rights.

4.5.5 regularly review and confirm that accounts provide the required access to each system. Whereas it is possible to have one account that can access many systems, this should only be implemented where:

4.5.5.1 each of the systems is at the same security level – see 3.3;

4.5.5.2 the controls in each system are designed to work this way;

4.5.6 ensure that passwords for user accounts meet the guidelines set out in Appendix C;

4.5.7 ensure the confidentiality of passwords for accounts when distributed to the users;

4.5.8 ensure that when a user terminates their employment with the Council their individual accounts are cancelled.

4.5.9 ensure that when a user terminates their employment with the council, all shared accounts the user was a member of are cancelled and a new account provided. Where this is not feasible, the ICT provider must ensure that the password on the account is forcibly changed;

4.5.10 ensure that when a user takes an a new role within the Council, that the account is updated to reflect the new requirements (ensuring the old requirements are removed)

4.5.11 ensure that if a user account is subjected to three login failures in succession, that the account is disabled. Where administrative accounts are used, the account disablement should not be implemented as it may render the system inaccessible.

4.5.12 ensure members of the administrator groups are authorised by the nominated system owner (usually a Service Centre Manager), the ICT Manager and Internal Audit;

4.5.13 if possible set an expiry date on all accounts. This is especially so for temporary staff accounts, as the duration and duties of temporary staff tend to be poorly understood, and can change significantly;

4.5.14 ensure that all administrator and specialist account passwords are securely stored, but accessible in emergency;

4.5.15 ensure that all default accounts and passwords for new assets are changed and preferably removed.

4.5.16 regularly review and confirm that all account information is current, and that the controls underpinning the accounts continue to meet the Council's needs

4.5.17 ensure that where a password reset is requested, that the requestor of the change is verified, and that the requestor has the authority to request the reset.

4.5.18 Where passwords are reset, the new password is only known to the ICT Provider and the requestor and that the requestor is changes the password on first use.

4.6 ICT Service Continuity

ICT Service Continuity is often known as Disaster Recovery. The SHDC Council policy is based on the ITIL guidelines, where the ICT Service Continuity is driven by the Business Continuity Strategy, resulting in a number of specific plans, the main ICT one being the ICT Recovery Plan. The ICT provider must:

4.6.1 provide and maintain the ICT Recovery Plan;

4.6.2 regularly review and test this plan, taking into account changes in technology and the business needs;

4.6.3 provide education, awareness and training for all staff who may be involved in a recovery.

This document supports the ICT Recovery plan in that it recommends the ICT provider:

4.6.4 ensures data backups are regularly completed, with a frequency to meet the requirements of the business users of each system. At least one backup copy for each system must be stored at a remote site. The currentness of the offsite copy must be agreed as part of the ICT recovery plan;

4.6.5 must have a **documented** and auditable data backup process for all systems – for third party systems, the suitability of the backup approach must be confirmed. The documentation must include:

- who is responsible for checking that backups can be correctly restored;
- where each backup is held and its status;
- a detailed description of the utilities that are used to restore data for applications. (e.g. Operating System, Data files, Databases);
- a detailed description of how to restore the Systems from the backups;

4.6.6 ensures the risks to the stored backups are understood and mitigated, including:

4.6.6.1 sensitivity/confidentiality of the data held within the backup;

4.6.6.2 susceptibility to environmental conditions when stored (humidity and ambient temperature);

4.6.6.3 risk of fire, flood or loss of access to the storage container;

4.6.7 ensures the backup solutions meet the recovery requirements, both in timescale and technology – if a third party recovery specialist is used, the ability of this third party to restore the backup data must be proven and regularly reviewed;

4.6.8 identifies Single Points of Failure (SPOFs), and where appropriate provide either redundancy in the infrastructure solution, or provide

hot-standby spares, which are maintained at the production level (configuration and software level).

4.7 Change Management and Release Management

ICT systems frequently need changes to be carried out to hardware, software and processes. A foundation to successful ICT Service Management is the systematic deployment of change and release management disciplines (see I.T.I.L. guide). The key aspects of these that impact security are:

4.7.1 all changes must be authorised. Some types of 'standard change' will be authorised once and can then be carried out many times without requiring a re-authorisation;

4.7.2 all changes must be documented (with a unique reference), with an audit trail of what was carried out, when and by who;

4.7.3 all changes must consider the impact of the change to both the other ICT systems and the users of the ICT systems;

4.7.4 the risk of the release must be understood and appropriate risk mitigation should be evaluated, including:

4.7.4.1 thoroughly testing the change on a non-production system/area, carrying out technical, business and data integrity testing;

4.7.4.2 planning the release of the change to have the least impact to the users and to provide time to overcome unforeseen issues;

4.7.4.3 provision of a "roll-back" solution if the release was unsuccessful;

4.7.4.4 ensuring that qualified ICT staff implement the release, and where external vendors carry out the updates, this should be under the supervision of qualified ICT staff.

4.7.4.5 ensuring that key technical and business staff are available both during and after the release.

4.8 Server Management

The Servers are usually key computers that provide ICT services to multiple other computers / users. The ICT provider:

4.8.1 should apply recognised upgrades/'patches' to keep the Servers current and to ensure security vulnerabilities are removed. This must be under change control – see 4.7;

4.8.2 should ensure servers are held in a secure and controlled environment, and in particular must be connected to a protected power supply – see 4.2;

4.8.3 must label the Servers and their peripherals to quickly identify them, and provide key data, for example IP Address;

4.8.4 should provide quickly accessible documentation of the networks ports the Servers are attached to;

4.8.5 ensure security controls on the servers have been implemented, and that ALL default passwords and accounts have been assessed and preferably removed;

4.8.6 ensure an agreed virus checking approach is in place;

4.8.7 ensure the integrity and availability of key services running on the servers, including:

- 4.8.7.1 databases;
- 4.8.7.2 file systems;
- 4.8.7.3 printing;
- 4.8.7.4 network lookup services (DNS, WINS, DHCP,NTP), ensuring they are not poisoned from external accidental or malicious activities;
- 4.8.7.5 e-mail and internet;
- 4.8.7.6 virus scanning;
- 4.8.7.7 specialist user software services;

4.9 Network Infrastructure Management

The network is both a hardware infrastructure, and the mechanism that allows ICT equipment to communicate / integrate. This section covers the physical infrastructure, 4.9 cover the connection point between different networks, 4.10 covers access management to external network services, and 4.11 covers the local area network device management and 4.12 covers the provision of user authentication to the network

The ICT provider must:

4.9.1 ensure the network topology is documented, including:

- 4.9.1.1 cable routes, including emergency links;
- 4.9.1.2 type of link: current speed; fibre/copper/wireless;
- 4.9.1.3 network components (Switches/hubs/Firewalls etc);
- 4.9.1.4 classification of network segments (internal, DMZ or external);
- 4.9.1.5 sub-net addressing scheme in use;
- 4.9.1.6 IP/IPX and MAC addresses of all addressable items;
- 4.9.1.7 Filters/features in use (ARP, QOS, Broadcast throttling, trunks, firewall rules …);
- 4.9.1.8 key network services (DNS, WINS, Proxies, Time Servers, DHCP, BootP, Firewall, management/monitoring stations, security authentication)
- 4.9.1.9 management access configured: management stations; types of access (telnet/snmp/web/proprietary); passwords.

4.9.2 ensure key network cabling is not be routed through publicly accessible areas, and is protected when taken through office accommodation;

4.9.3 where possible use routers and switches in preference to hubs. Apart from reducing the load on the infrastructure, they make it much harder to intercept network data;

4.9.4 when new unknown equipment is to be connected to the LAN, this should be setup in a test segment to ensure it is compatible with the network and can be fully configured before being attached to the production LAN.

4.9.5 ensure that the system software used by connecting devices is compatible with the ICT infrastructure.

4.9.6 keep regular backups of the settings/configuration of network infrastructure components;

4.9.7 consider the threat of electromagnetic eavesdropping, and where appropriate shield/encrypt the data;

4.9.8 ensure that all wireless devices use strong encryption (128bit+);

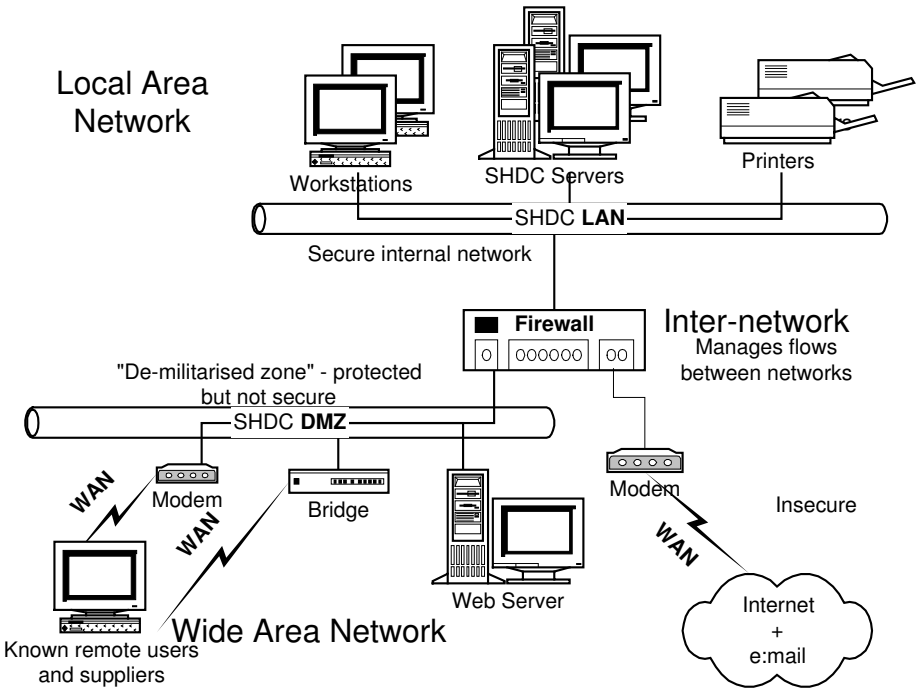
4.9.9 provide a mechanism to de-activate network ports when not required, preferably automatically (for example time of day);

4.9.10 ensure all equipment is maintained with the latest recognised patches/firmware upgrades, following the change process (4.7);

4.9.11 configure network devices to stop inappropriate re-configuration. This may involve a combination of password and address based security, either in the device itself or in some cases in an external device that can provide this security. Community names used in SNMP management must be changed from “public”, and unless necessary, SNMP write access should be disabled;

4.9.12 configure the SHDC LANs and DMZ to use an IP address range that is not externally accessible (10.x.x.x, 192.168.x.x)

4.9.13 should ensure key network assets are held in a secure and controlled environment, and in particular must be connected to a protected power supply – see 4.2;



4.10 Inter-network Connection Management

This section refers to both the devices that manage the inter-network connection and the devices in the Demilitarised Zone (DMZ). The ICT provider must:

4.10.1 implement firewalls wherever external networks need to connect to the Council LAN;

4.10.2 ensure all network equipment is ‘hardened’ to provide only those services that MUST be available to meet the Council requirements;

4.10.3 ensure that network equipment can only be administered from known management stations within the LAN. If possible, filtering

should be in place to stop any external access to the management ports, to minimise the risk of a Denial Of Service attack;

4.10.4 ensure all traffic between the networks is routed through the firewalls – this includes all network traffic that did not originate in the Follaton SHDC LAN.

4.10.5 provide a policy document for each connection to a firewall detailing the purpose of the connection and agreed usage;

4.10.6 configure the firewalls to:

4.10.6.1 initially block all network protocols to all addresses;

4.10.6.2 not respond to port scanning, for example Ping, so as to minimise the amount of information that an external probe can ascertain about the Council network;

4.10.6.3 to have ALL default accounts / passwords changed, see section 3.3;

4.10.6.4 provide web services (ports 80 and 443), where routed through the Web proxy server;

4.10.6.5 provide FTP services where routed to the Web proxy server;

4.10.6.6 provide FTP services where routed between the LAN and DMZ;

4.10.6.7 block ALL traffic if the firewall device fails;

4.10.6.8 detect and block spoofing of network packets;

4.10.6.9 provide access to LAN and DMZ addresses through address translation on an individually agreed basis;

All other changes must be agreed through the change management process, and must be based on the premise that minimum access should be provided for specific purposes/users;

4.10.7 document the current firewall configuration and backup the settings;

4.11 Wide Area Network Connection Management

This section covers the management of services to and from the WAN. The ICT provider must:

4.11.1 implement link encryption and verification where connecting to remote trusted locations (for example other SHDC sites);

4.11.2 where confidential or critical information needs to be transferred, implement mechanisms to verify the identity of the remote connection. For incoming connections, this should include Caller Line Identification (CLI). The quality of the transfer should also be guaranteed through the use of integrity checks (for example CRC);

4.11.3 manage access to the Internet through user authentication;

4.11.4 other than for insecure services (http to the Web server and SMTP to the Mail Server), ensure incoming connections are authenticated through challenge-response encrypted mechanisms. The use of one-time passwords, usually time dependent (for example a Radius system) should be required where the incoming connection will be given access to internal SHDC systems;

4.11.5 where applicable, use call-back authentication;

4.11.6 all inbound and outbound traffic to be actively filtered for:

4.11.6.1 known and potential viruses;

4.11.6.2 unapproved file types;

4.11.6.3 potentially offensive material;

4.11.6.4 blocked internet sites and activities (for example web based e-mail services);

Due to the frequency of viruses being released, multiple virus checkers (preferably three or more) from different vendors should be used.

4.12 Local Area Network Connection Management

This should be the most secure part of the network, and therefore all connections to the LAN should not compromise this status. To ensure this, the ICT provider must:

4.12.1 avoid implementing solutions that rely on workstations with directly connected modems. Where these are unavoidable, then the use of these should be strictly managed, both in terms of the initial connection and the activities undertaken whilst the connection is ongoing;

4.12.2 ensure that no unauthorised network connection occurs to the LAN;

4.12.3 provide LAN based virus checking on all devices that attach to the LAN that can potentially infect of become infected. The virus checking solution must be regularly updated;

4.12.4 ensure that without suitable access accounts, the current workstations and peripherals do not permit access to the LAN. Microsoft Windows NT and XP professional are the Council standard for workstations as they contain a relatively high level of security controls.

4.13 Local Area Network User Access Management

The primary purpose of the SHDC LAN is to allow users to access shared resources. To enable this the ICT provider must implement a mechanism to allow users to access workstations where:

4.13.1 the user is provided only those applications that they are approved and licensed to use;

4.13.2 work related files are retrieved and stored in the central file server, rather than on the local disk space. The storage area on the

central file server will be allocated dependent on the access rights of the user account;

4.13.3 the workstations environment, including icons, menus, colour schemes etc will be managed to ensure the work station is not compromised;

4.13.4 executing files (*.exe *.com *.VBS *.BAT …) other than those provided will be blocked;

4.13.5 unnecessary drives, including local hard drives, CD-ROM, Floppy diskette and USB are disabled;

4.13.6 a screen timeout (set to 15 minutes) is implemented to secure the workstation where the user leaves the workstation unattended;

4.13.7 simultaneous logins at different workstations can be controlled or stopped;

When a user logs on to the LAN, the following information should be displayed:

4.13.8 a legal notice informing the user of implications of system abuse;

4.13.9 the time and device of last successful and unsuccessful login (user should check that they are correct);

4.14 Proactive asset monitoring and management

To ensure that the Council's ICT assets meet the needs of the Organisation, it is necessary to the both monitor and manage the operation of the ICT assets. The monitoring can be both active (probe the devices) and passive (recording information initiated from the devices).

4.14.1 The ICT provider must deploy mechanisms to monitor the ICT assets, covering in particular:

- 4.14.1.1 current utilisation of key network infrastructure;
- 4.14.1.2 current utilisation of Server resources;
- 4.14.1.3 current availability of key resources (servers, software, network);
- 4.14.1.4 utilisation of software licenses;
- 4.14.1.5 unsuccessful login attempts;
- 4.14.1.6 suspicious network activity, especially at the firewalls;
- 4.14.1.7 recording of all non-information errors raised by assets;
- 4.14.1.8 unsuccessful updates of Virus checking software;
- 4.14.1.9 virus alerts where potential viruses are detected;
- 4.14.1.10 scanning for unauthorised equipment;

4.14.2 The ICT provider must implement processes and procedures to utilise the monitoring data so it can be used to drive management activities. This should include:

4.14.2.1 filtering all monitoring data to remove irrelevant items. this filtering should be documented;

4.14.2.2 raising incidents for all other items;

4.14.2.3 implementing alerting mechanisms to highlight high priority incidents to the appropriate ICT staff;

4.14.2.4 investigating all incidents to find the underlying cause, and taking appropriate action to resolve the incidents. This is documented in the ITIL Incident and Problem management processes;

4.14.3 The ICT provider must carry out regular reviews of the monitoring and subsequent activities to ensure these meet the needs of the Council;

4.15 System development and third party product selection

All new or updated assets that are introduced to the ICT infrastructure must be assessed against for compatibility with the ICT infrastructure and this Security policy - see (4.1). In addition and as re-enforcement to the other sections in this policy, the ICT provider who implements or selects products must:

4.15.1 avoid the use of products that require direct attached modems or other devices that cannot be directed through the ICT firewalls;

4.15.2 ensure that application & system configuration files are protected against accidental or malicious corruption, and must not be readable to other users.

4.15.3 where errors occur in the product, these should be written to standard logs, which can then be routed to the central logging system. This includes NT Eventlogs and Unix Syslog.

4.15.4 ensure databases are secured against accidental or malicious viewing or updating. This should be accomplished by:

4.15.4.1 ensuring all databases are password protected;

4.15.4.2 deploying verification mechanisms to ensure databases are only updated by particular authenticated systems;

4.15.4.3 not providing tools or applications to users that let them update product databases without using the product itself;

4.15.5 understand the type of data to be managed by the product, so as ensure appropriate controls are in place to manage access, for example personal data;

4.15.6 Time dependent processes must ensure that the time used is accurate, either through the use of the Server system clock, or by direct access to the ICT time server;

4.15.7 ensure that if the product is to maintain it's own controls, account and password system, that it meet the needs of the security policy. In particular:

4.15.7.1 the controls must provide the granularity required by both the Council users and Internal Audit;

4.15.7.2 the maintenance of user accounts should only be accessible to users who have access to an administrator account for that product;

4.15.7.3 password must be stored with strong encryption (one way) algorithms;

4.15.7.4 passwords must never be displayed on screen, or passed across the network in an unencrypted format;

4.15.7.5 all access to the product and key updates should be logged to a secure audit log;

4.15.7.6 administration tools should be provided to access the audit logs and provide account and control based information;

4.15.7.7 **Ensure that the message displayed during a failed logon is identical whether the logon failure was due to the wrong account or password being entered;**

Where possible, the use of industry standard strong password authentication should be used, for example Unix or Windows NT;

4.15.8 ensure that product source code and configuration data is available to:

4.15.8.1 allow the product to be rebuilt

4.15.8.2 provide earlier versions of the product where there is the need to process backup data, including where there is the need to provide evidence for internal and external audits

4.15.8.3 ensure that if a third party supplier fails, that the Council has access to the last copy of the code (key escrow)

4.15.9 ensure that the development of products:

4.15.9.1 is carried out in a separate development/test environments;

4.15.9.2 uses test data that is free from personal or confidential data;

4.15.9.3 be developed in a computer language and style that can readily be maintained by more than one developer;

4.15.9.4 be fully documented.

4.16 Miscellaneous requirements

4.16.1 A non-disclosure agreement should be signed by external parties accessing the SHDC infrastructure, ensuring that neither details of the interface, nor data accessible via the interface may be disclosed to third parties.;

4.16.2 A non-disclosure agreement should be signed by staff and in particular ICT provider staff who have access to administrator account information;

4.16.3 To reduce the risk of key updates being carried out whilst it is in use, a maintenance schedule should be agreed with the ICT infrastructure users, where for example once a month the system is unavailable for use a particular evening between 19:00 and 21:00;

4.16.4 Specialist encryption keys that are registered to the Council, and have a legally binding status must be kept secret. The ICT provider must demonstrate to Internal Audit the management of these keys.

4.17 Accountability and audit

To ensure the Management, the Users and the ICT providers are meeting the requirements of this policy, it is necessary for the ICT provider to record and when necessary provide information to both internal and external audit for regular audits against this policy.

4.17.1 To meet this requirement, the ICT provider must keep a minimum of one years records for the following:

- 4.17.1.1 e-mail contents;
- 4.17.1.2 internet usage and content;
- 4.17.1.3 a log detailing the login account, time of login and workstation used, and when the account was logged off;
- 4.17.1.4 external connections activities to the SHDC network;
- 4.17.1.5 firewall logs;
- 4.17.1.6 external or analogue line that might be being used for a modem;
- 4.17.1.7 provide a quarterly report of incidents, and actions taken to resolve them;
- 4.17.1.8 maintenance records for assets and the environmental controls;
- 4.17.1.9 provide a monthly report of all access accounts defined in the ICT systems and the users and/or use of each, being prepared to demonstrate the authorisation for them;
- 4.17.1.10 provide a quarterly report of all change requests that relate to ICT assets;
- 4.17.1.11 where possible provide a log of system administrator activities;
- 4.17.1.12 anything else that the ICT provider feels may be necessary to demonstrate their compliance with the requirements of this policy;

4.17.2 To support the management of these records, the ICT provider must:

4.17.2.1 protect audit logs and utilities from unauthorised use or tampering

4.17.2.2 ensure all logging systems have their clocks synchronised to guarantee the validity of audit log timestamps.

4.18 Security Breach Management

Even with a solid security policy, educated users and solid system administration, a *major incident* response team is useful, as a quick response is a requirement for systems critical to the functioning of the Council. See ITIL guidelines for details on the handling of Major Incidents.

All such incidents must be formally recorded and investigated.

Appendix A – Acceptable use

SHDC Acceptable Use of ICT equipment, the internet and e-mail,

These rules apply to everyone and are in place to ensure that the investment the Council has made in Information Technology is in no way compromised by its inappropriate use.

For the authorative version please refer to the latest version on the SHDC Intranet on:

http://www.south-hams.gov.uk/it/Policies/use_of_computer_equipment.htm

Council ICT equipment

- No software may be loaded onto a computer from either floppy disc, CD, Internet download or any other method, without the express permission of the ICT section. Under normal circumstances, software should only be loaded by the ICT Section. If in any doubt, please contact the ICT Section for clarification.
- Access to computer systems should only be made using your own login and password. You must not use anyone else's password or disclose your own. Passwords should not be written down; put on the wall; kept in your drawer etc. If you feel your password has been compromised, you should change it straightaway by contacting the ICT Section.
- To ensure the compatibility, suitability, cost effectiveness, maintainability, security and safety of ICT equipment, the ICT Section are responsible for the procurement, installation and subsequent relocation of Council Owned ICT equipment.

Internet and e-mail

The Policy contains important rules and guidelines covering e-mail and Internet access. This Policy explains how e-mail and Internet access should be used and explains what you are allowed and not allowed to do. The Policy is to ensure that SHDC as an authority is not exposed to either civil or criminal action that would bring the authority in to disrepute or have a financial penalty.

Failure to comply with the rules set out in this Policy:

- may result in legal claims against you and the Council; and
- may lead to disciplinary action being taken against you.

It is sensible to ensure that all members of staff are informed that the items listed in the **Don't** section will constitute **'misuse'**.

If there is anything that you do not understand, it is your responsibility to ask your line manager or the ICT section to explain.

General Rules

Do ……

- Observe this policy at all times and note misuse will be subject to disciplinary action in accordance with the authorities disciplinary procedure, which may include gross misconduct and lead to dismissal;
- Ensure that all e-mail, whether sent or received, are treated as material documents and appropriate steps are taken to provide that, like letters, they are placed on the appropriate file or record;
- Ensure that, if you are a member of a profession you comply with all the standards relating to e-mail set down by that body;
- Appreciate that the Council will routinely monitor incoming, outgoing, and internal e-mail and internet usage to ensure compliance with this policy. You should not therefore assume that your e-mails are private;

Don't ……

- Send any message, internally or externally, which are potentially libellous, abusive, intimidating, hostile or humiliating;
- Visit, view, download or send any material containing sexually explicit, obscene, illegal, or any other highly offensive content;
- Transmit any personal or confidential information of the council;
- Subscribe to any e-mail mailing lists, web forums or newsgroups without the consent of your Service Centre Manager or Chief Officer;
- Use the Councils e-mail or internet systems for private purposes except on a strictly occasional basis. For the avoidance of doubt, five or less incoming and outgoing e-mails per week is considered occasional;
- Download or send any material which is the copyright or otherwise the property of a third party unless you have agreement to do so;
- Access any personal internet based e-mail accounts (e.g. Hotmail, Yahoo, etc.) via the Council's internet system;
- Set up rules on your Council e-mail account that forward e-mail to a personal account elsewhere. This could result in personal or confidential information leaving the Council in an insecure environment;
- Impersonate any other person when using e-mail or amend messages received.

Other Guidelines

- Avoid congesting the e-mail system by not sending trivial or personal messages or by copying e-mails to those who do not wish to see them;

- Virus warning e-mails are generally hoaxes and should be forwarded to the IT Service Desk only. Do not forward the e-mail to everyone in your address book (as the e-mail may advise you to do) as this will create unnecessary congestion;
- If you are based at a remote site without a connection to the Council network, do not open attachments without first obtaining the latest virus update files;

Please note:

All members of staff are reminded the above list is not exhaustive and as technology advances other misuse of similar gravity could also constitute a disciplinary breach.

Appendix B - Data and Information Classification

For use in SHDC, information must be classified into five types:

1. Public Information
Data on these systems could be made public without any implications for the Council (i.e. the data is not confidential or commercial). Examples include dates of public events, public contact details issued by the Council, public communication documents once they have been authorised for distribution for the public.

2. Internal Information
External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. the Council may be publicly embarrassed, but will not significantly interrupt the functioning of the Council). Internal access is selective. Examples of this type of data are found in certain "normal" working documents and project/meeting and internal telephone books.

3. Confidential Information
Data that is classed as highly sensitive or is confidential within the Council and should be protected from external access. If such data were to be accessed by unauthorised persons, it could influence the Council's operational effectiveness.

4. Personal Information
The definitive definition of this is covered in the Data Protection Act 1998. For the purpose of the security policy, this type of data should be treated as Confidential Information.

5. Sensitive Personal Information
The definitive definition of this is covered in the Data Protection Act 1998. For the purpose of the security policy, this type of data should be treated as Confidential Information.

Appendix C - Guidance creating a secure password

Television Programmes such as BBC's Tomorrow's World have demonstrated how easily expert security consultants can acquire passwords just from basic background information checks and the content of a persons office. On top of this, with the increasing speed of computers and the available of easily downloadable hacking tools, simple dictionary and common password lists can be used to crack passwords in minimal time where the password is a simple word or expression. The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you've chosen. This leaves them no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation.

The guidance below suggests ways to improve the security of passwords.

Content

- Choose a line or two from a song or poem, and use the first letter of each word.
- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily remembered.
- Choose two short words and concatenate them together with a punctuation character between them.

Bad Examples

- Don't use your login name in any form.
- Don't use your first or last name in any form.
- Don't use your spouse or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, national insurance numbers, the brand of your car, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

Good Examples

- Do use a password with mixed-case alphabetic characters.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Appendix D – Security policy overview

Key responsibilities of SHDC IT users:

DO'S!

- ☺ Keep your passwords a secret, if you suspect that your password has been revealed to anyone, please inform the IT Section immediately;
- ☺ Keep your passwords cryptic! Mixing numbers with uppercase and lowercase letters increase the security of the password. (i.e Bat1Ball2);
- ☺ Passwords need to be changed regularly for security reasons, the system will prompt you regularly for the required password changes
- ☺ If you are made aware of or receive any e-mails with viruses attached, 'get rich quick' schemes or unwanted e-mails please inform the IT section;
- ☺ Protect our Data! Documents need to be protected – they can be damaged, lost or stolen. In all possible cases please save all council documents to the L: or U: drives;
- ☺ Switch your pc's off at the mains when leaving work, not only does it reduce the fire risks it also saves electricity;
- ☺ When borrowing a laptop, ensure it stays in the case provided when travelling, it will protect the equipment. Also remove any media from the drives when not in use;
- ☺ When working with non-council representatives, ensure that your screen is not visible to them where the data could be confidential or personal;
- ☺ Avoid eating or drinking near pc equipment.

DONT'S

- ☠ Do not: use the council's computer equipment for personal use;
- ☠ Do not: write your passwords down!
- ☠ Do not: disclose your passwords to anyone, including IT staff;
- ☠ Do not: use passwords that can be linked to you personally (i.e names of family members or pets.);
- ☠ Do not: re-use previous passwords;
- ☠ Do not: download any programs from the internet. As well as licensing laws external software also carries a virus risk!
- ☠ Do not: directly purchase any PC equipment or accessories (including digital cameras) - all IT purchases must be requested through the IT section. This ensures compatibility with existing equipment, insurance, and also uses the buying power of the IT section to get the best price … it's also a disciplinary offence to go directly !
- ☠ Do not: allow anyone to loan borrowed IT equipment, or disclose laptop passwords to anyone;
- ☠ Do not: allow anyone to connect non-approved IT equipment to Council ICT equipment. Contact the IT Service Desk if this is a requirement.
- ☠ Do not: dispose of any sensitive (personal or confidential) material (including media disks) in the waste bins, please treat the information as confidential waste;

Please note this is only a short user-guide please refer to full document for further information: Insert link here